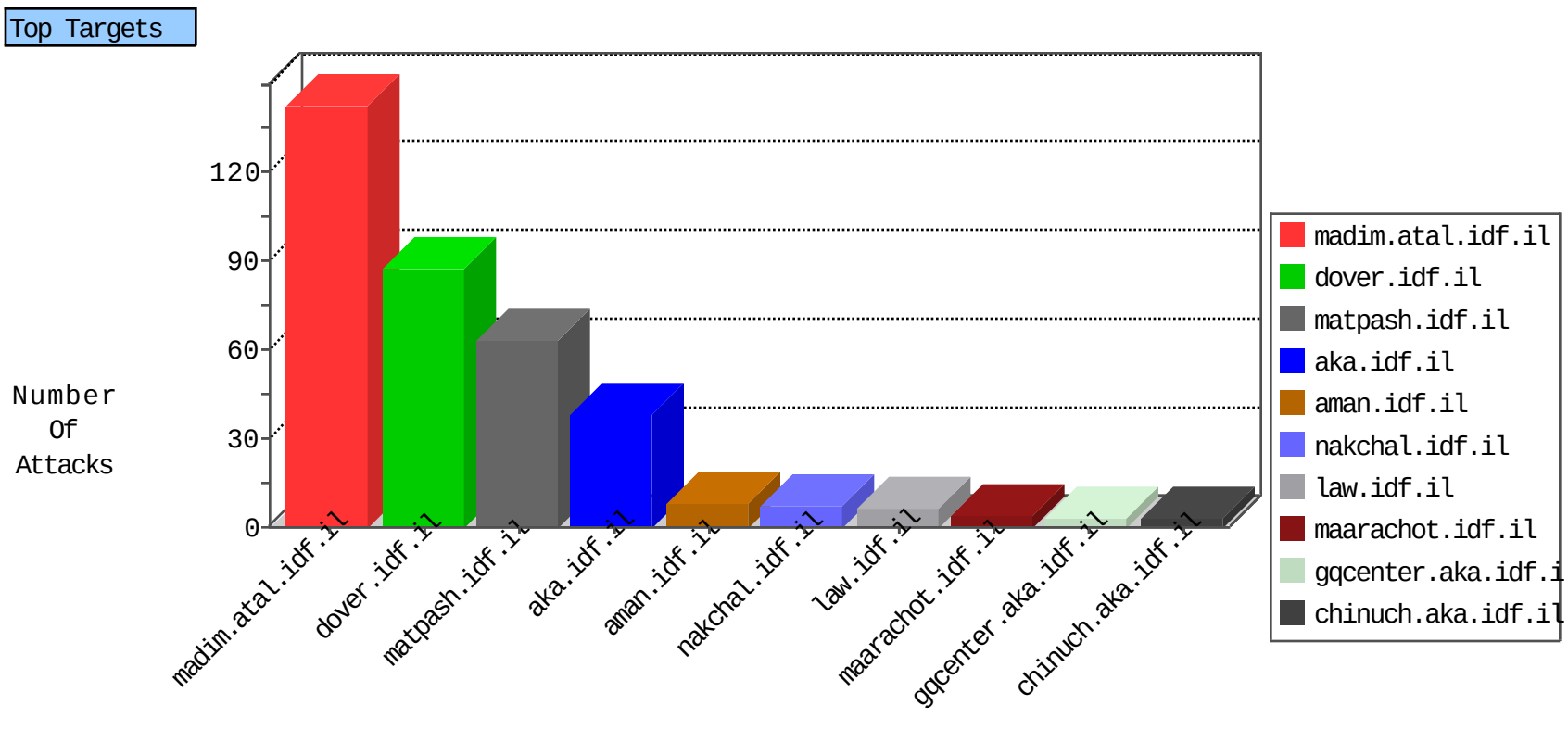
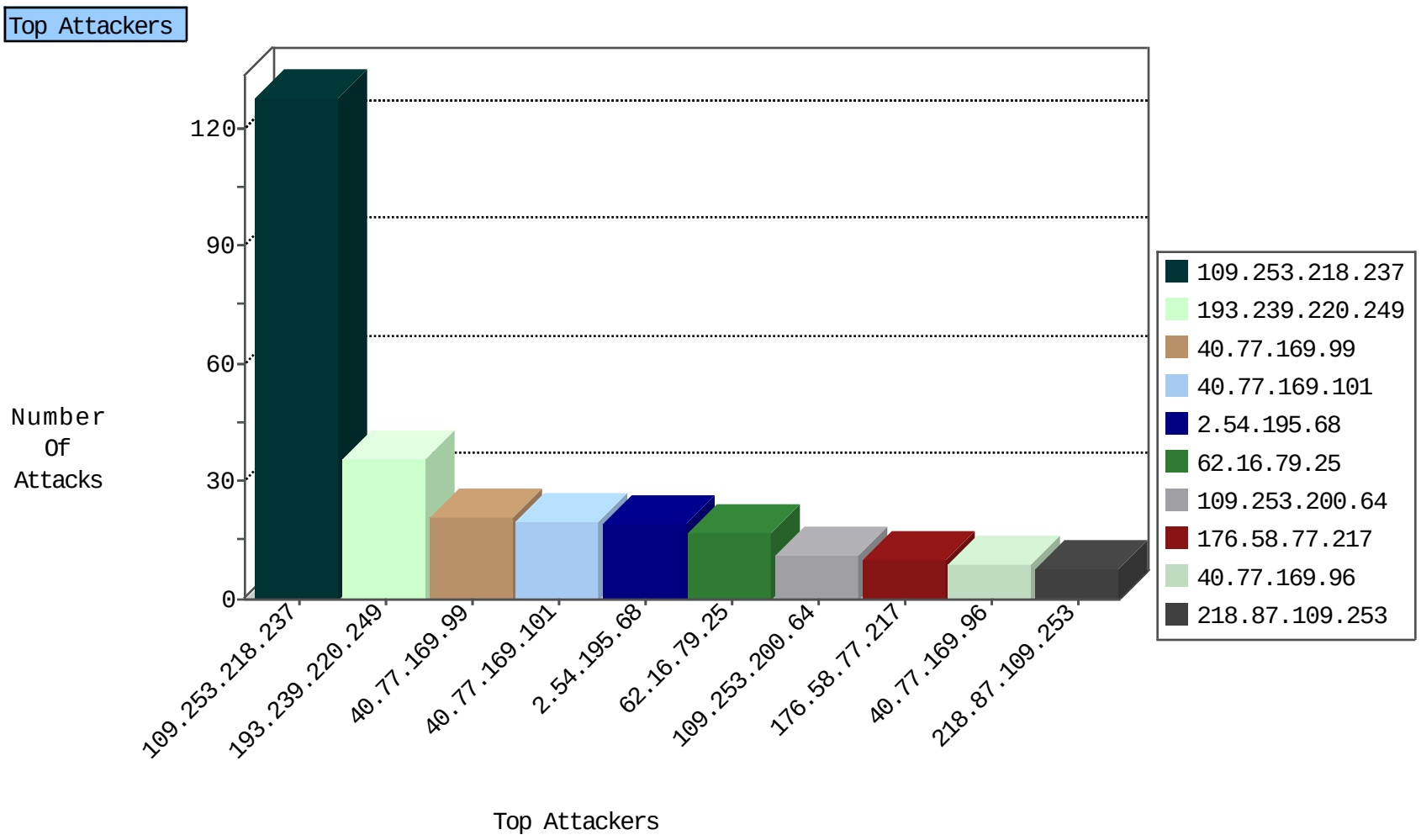
08-25-2016-17:04:00 to 08-25-2016-18:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-25-2016-17:04:00 to 08-25-2016-18:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.0.168	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
94.23.80.118	Spain	147.237.76.198	e.yohalan.idf.il	Black List	drop	1

08-25-2016-17:04:00 to 08-25-2016-18:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
71.6.167.142	United States	147.237.76.202	e.halag.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
93.115.95.206	Anonymous Proxy	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1
151.80.31.108	France	147.237.76.147	chinuch.aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

08-25-2016-17:04:00 to 08-25-2016-18:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
91.224.160.106	147.237.76.148	Netherlands	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
87.236.194.161	147.237.76.148	Czech Republic	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
66.203.215.242	147.237.8.14	Canada	e.orchot.idf.il	ET SCAN NMAP -sS window 3072	1
218.87.109.253	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
66.203.215.242	147.237.8.14	Canada	e.orchot.idf.il	ET SCAN NMAP -f -sS	1
218.87.109.253	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
37.26.146.207	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.87.109.253	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
123.206.73.185	147.237.76.34	China	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
97.105.173.114	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
79.178.48.73	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	1
66.203.215.242	147.237.8.14	Canada	e.orchot.idf.il	ET SCAN NMAP -sS window 2048	1
218.87.109.253	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
46.227.67.172	147.237.8.45	Sweden	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
218.87.109.253	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	1
18.85.22.237	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	1
218.87.109.253	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
106.186.20.183	147.237.76.31	Japan	nakchal.idf.il	ET SCAN Potential SSH Scan	1

08-25-2016-17:04:00 to 08-25-2016-18:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
193.239.220.249	Switzerland	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	36
2.54.195.68	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
40.77.169.101	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	19
62.16.79.25	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	13
40.77.169.99	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	12
176.58.77.217	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
40.77.169.96	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	9
40.77.169.99	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	9
40.77.169.103	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	7
46.19.86.218	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
59.96.26.161	India	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	2
59.96.26.161	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
176.13.224.62	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	2
62.16.70.7	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
59.96.26.161	India	147.237.76.147	chinuch.aka.idf.il	drop	First packet isn't SYN	drop	2
62.16.79.25	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
169.229.3.91	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
176.13.16.57	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	1
100.92.23.134		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.77.212	e.dover.idf.il	drop	SAM rule	drop	1
109.64.115.114	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	1
176.13.9.24	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
178.92.46.58	Ukraine	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.77.19	law-forum.idf.il	drop	SAM rule	drop	1
176.13.11.64	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
40.77.169.101	United States	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	1
183.129.160.229	China	147.237.76.176	test.ncore.idf.il	drop	SAM rule	drop	1

08-25-2016-17:04:00 to 08-25-2016-18:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.218.237	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	128
109.253.200.64	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	11
31.154.81.54	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	4
77.138.207.244	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/kiosk	Block	3
176.13.10.21	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
31.210.186.69	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
40.77.169.100	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
40.77.169.102	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
84.111.60.49	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
46.19.85.229	Israel	147.237.77.74	law.idf.il	Multiple Illegal HTTP Version from 46.19.85.229	Block	1
207.46.13.109	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
31.154.81.54	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/sip_storage/files/2/	Block	1
98.139.14.250	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/giyus/general/	Block	1
77.138.103.48	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	1
40.77.169.100	United States	147.237.77.170	maarachot.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
5.29.181.69	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
157.55.39.37	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
85.64.246.196	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/589-he/patzar.aspx=	Block	1
46.19.85.229	Israel	147.237.77.74	law.idf.il	Multiple Malformed URL from 46.19.85.229	Block	1
212.179.104.26	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	1
24.24.146.192	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
157.55.39.181	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_bottom.asp	Block	1
85.250.136.95	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.85.229	Israel	147.237.77.74	law.idf.il	Multiple Unknown HTTP Request Method from 46.19.85.229	Block	1
212.179.104.26	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/wp-login.php	Block	1
37.142.196.29	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
79.179.133.202	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
157.55.39.229	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/smalim/smalim.aspx	None	1
87.69.73.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/0/	Block	1
66.102.9.176	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
37.142.206.156	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
114.98.232.180	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/home/default.aspx/trackback/	Block	1
84.111.25.91	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
46.19.85.150	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
31.154.81.54	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 31.154.81.54	Block	1
93.172.248.27	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.240.192.138	United States	147.237.77.235	sviva.idf.il	Unauthorized URL Access to 147.237.77.235/robots.txt	Block	1
40.77.169.98	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
5.29.181.69	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 5.29.181.69	Block	1
131.253.27.23	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1

08-25-2016-17:04:00 to 08-25-2016-18:04:00